Firmware Release Note

ZyAIR G-5100

Release 3.50(HV.1)C0

Date: May 18, 2005
Author: Chin-Te Huang

ZyXEL ZyAIR G-5100 Standard Version

release 3.50(HV.1)C0

Release Note

Date: May 18, 2005

Supported Platforms:

ZyXEL ZyAIR G-5100

Versions:

ZyNOS Version : V3.50(HV.1) | 05/18/2005 17:48:15
Bootbase Version : V1.03 | 08/30/2004 16:28:56

Notes:

1. ZyAIR G-5100 is a country dependent product. Please setup correct country code before shipping.
2. uAP code is version 1.2.8.0
3. When using internal RAIDUS server with MD5 in G-5100, STA can still connect to G-5100 with PEAP configuration which disable dynamic WEP key. If the setting is PEAP with dynamic WEP key disabled in G-5100, STA can use MD5 to connect to G-5100

Known Issues:

1. WinXP supplicant doesn't work when it configures as 802.1x authentication with static WEP key.
2. WPA interoperability issue : When centrino station configure as WPA (or WPA-PSK) mode and data encryption filed set as WEP, it can not work with G-5100 under WPA (or WPA-PSK) mode and using WEP as group key. In this case, user must configure the data encryption field as TKIP then stations will automatic switch the group key cipher as WEP after it received the WPA information element from G-5100.
3. WDS links will be broken temporarily with heavy traffics.

4. Sometimes system exception occurred when configuring the WLAN or 802.1x/WPA/WPA-PSK settings.
5. CNM support is not ready.

CI Command List:

Features:

Modification in 3.50(HV.1)C0 | 18/05/2005

1. [FEATURE CHANGED]
   Change ZyNOS version from 3.50(HV.1)b1 to 3.50(HV.1)C0.

Modification in 3.50(HV.1)b1 | 12/05/2005

1. [BUG FIXED]
   System: After changing the DUT operation mode from "AP" to "AP + bridge", DUT doesn't forward wireless packet properly between 802.1X wireless STAs.

2. [BUG FIXED]
   System: 15 wireless STAs associate to DUT which is configured as AP only mode, more than 10 STAs can't access the DUT after 12 hours stress test even though user disable/enable the wireless card manually.

Modification in 3.50(HV.0)C0 | 07/04/2005

2. [FEATURE CHANGED]
   Change ZyNOS version from 3.50(HV.0)b5 to 3.50(HV.0)C0.

Modification in 3.50(HV.0)b5 | 01/04/2005

3. [FEATURE ENHANCED]
   Online help in eWC is ready.

Modification in 3.50(HV.0)b4 | 21/01/2005

4. [FEATURE ENHANCED]
   Support 2 WLAN adapters.

5. [FEATURE ENHANCED]
   Support VLAN feature.

6. [FEATURE ENHANCED]
   Support output power feature.

7. [FEATURE CHANGED]

Accounting process will be disabled in WPA-PSK mode, embedded RADIUS used, and Local user database used.

8. [BUG FIXED]
   Symptom: Domain name will be erased when changed IP address assignment from dynamic to static.

9. [FEATURE ENHANCED]
   Enhance WEP Key. (It shows WEP key value when users input the key; And replace the WEP key value with "*****" if browser refreshes.)

10. [FEATURE ENHANCED]
    Show WDS link status in Association List page

11. [BUG FIXED]
    Wireless -> MAC Filter : input incorrect MAC and the alert message is incorrect.

12. [FEATURE ENHANCED]
    Add product name to browser title of login / logout pages.

13. [FEATURE ENHANCED]
    Maintenance -> Channel Usage : max listing is 48

14. [FEATURE ENHANCED]
    Add warning message to Trusted User page : Password : Maximum 14 ASCII characters with PEAP.

15. [FEATURE ENHANCED]
    Extend VLAN tag setting range from 255 to 4094.

16. [BUG FIXED]
    WDS(Enable PSK):After overnight testing, FTP clients disconnect when running 6 AP+Bridge mode.

17. [BUG FIXED]
    STA can pass the authentication and access network when enable accounting server that didn't exist.

18. [FEATURE CHANGED]
    Remove duplicate message 'Switch to authentication server ip:127.0.0.1, port 1812' appear when run internal RADIUS server.

19. [BUG FIXED]
    Symptom: The default value of bridge RSTP port should be enabled in the ROM file that will cause WDS link disconnect when WDS topology has a loop existed.

20. [BUG FIXED]
    Symptom: System exception and reboot occur when system name is up to 30 characters long and enable 802.1x.

21. [FEATURE ENHANCED]
    When user associated and key handshake done, add log to identity user login type.

22. [FEATURE ENHANCED]
    Symptom: Enter special url will cause device crash.
    Condition: Form LAN site, enter http://192.168.1.1/Forms/rpAuth_1?ZyXEL%20ZyWALL%20Series<script>top.location.pathname=%20""</script> on browser, the device will crash.

Modification in 3.50(HV.0)b3 | 01/12/2004

23. [FEATURE ENHANCED]

Upgrade AP firmware from 1.0.4.3 to 1.2.8.0.

Modification in 3.50(HV.0)b2 | 27/10/2004

1. [BUG FIXED].
   Symptom : Internal RADIUS server with PEAP cannot work when STA enable 'validate server certificate'.

2. [BUG FIXED]
   Symptom : Internal RADIUS server cannot work when using ZyAIR G-560 as trusted AP.

3. [BUG FIXED]
   Symptom : The real fragmentation threshold should be higher than 800 in Conexant WLAN chip.

4. [BUG FIXED]
   Symptom : WPA-PSK: mixed mode selected item is not consistent between SMT and eWC.

5. [BUG FIXED]
   Symptom : Enter debug mode from SMT24.7.1 or SMT24.7.2 and type "atgo", system will hang.

6. [BUG FIXED]
   Remove a warning message for WLAN chip detection. in SMT

7. [FEATURE CHANGED]
   Change the default configuration of log settings. Now centralized log is enabled by default.

8. [FEATURE CHANGED]
   When 802.1x key management protocol is WPA-PSK, STA that configured as 802.1x with dynamic WEP key will not connect to G-5100.

Modification in 3.50(HV.0)b1 | 06/10/2004

1. First release for C3 firmware

Appendix 1 : CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
Wireless LAN Related Command	IP Related Command	Bridge Related Command
802.1x Related Command	Vantage Related Command	

System Related Command

Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	log			
		clear		clear log error
		disp		display log error
		online	[on|off]	turn on/off error log online display
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		save	[entry no.]	save remote node information
	stdio		[second]	change terminal timeout value
	systemname		[system name]	Change system name
	time		[hour [min [sec]]]	display/set system time
	trcdisp	parse, brief, disp		monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463

	romreset			restore default romfile
	socket			display system socket information
	filter			
		netbios		
	cpu			
		display		display CPU utilization

Exit Command

Home

Command				Description
exit				exit smt menu

Ethernet Related Command

Home

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type
	edit			
		load	<ether no.>	load ether data from spt
		save		save ether data to spt

Wireless LAN Related Command

Home

Command				Description
Wlan [0/1]				
	active		[on|off]	set on/off wlan
	association			display association list
	chid		[channel id]	set channel
	diagnose			self-diagnostics
	essid		[ess id]	set ESS ID
	scan			scan wireless channels
	version			display WLAN version information

IP Related Command

Home

Command				Description
ip				
	address		[addr]	display host ip address
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		stats		

	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	status			display ip statistic counters
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	telnet		<host> [port]	execute telnet clinet command
	tftp			
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group

Bridge Related Command

Home

Command				Description
Bridge				
	cnt			related to bridge routing statistic table
		disp		display bridge route counter
		clear		clear bridge route counter
	stat			related to bridge packet statistic table
		disp		display bridge route packet counter
		clear		clear bridge route packet counter

802.1x Related Command

Home

Command				Description
radius				
	showRunInfo			Show server running information.
	auth	show		show current radius authentication server configuration
		addAuthServer		Add an authentication server.
		delAuthServer		Delete an authentication server.
	acct	show		show current radius accounting server configuration
		addAcctServer		Add an accounting server.
		delAcctServer		Delete an accounting server.
8021x	debug	reauth	<0:off 1:on>	set IEEE802.1x reauthentication method
		level	[debug level]	set ieee802.1x debug message level
		trace		show all supplications in the supplication table
		user	[username]	show the specified user status in the supplicant

				table

Vantage Related Command

Home

Command				Description
cnm	active	[0/1]		Display or set the CNM features to enable or disable . 0: disable 1: enable CNM features and communicate through WAN interface.
	sgid			Display sgid which is the unique ID of the device in Vantage.
	managerIP	[addr]		Display or set the IP of Vantage server/COMServer which manage this device. [addr] specifies the IP of the Vantage serve/COMServer.
	debug	[0/1]		Display or set the way of outputting CNM debug messages. 0: disable debug messages. 1: output the debug messages to console and can accept SGMP inquire message only after the device is registered to Vantage server.
	reset			Reset the state machine of SGMP and return to the state of SGMP_STATE_UNKNOWN. Device will re-register to Vantage server if CNM is active.
	encrykey	[string]		Display or set encryption key. [string] specifies the encryption key. to be set. Key length can not less than 8 alphanumeric characters long, if ecrymode is DES. Key length can not less than 24 alphanumeric characters long, if ecrymode is 3DES.
	encrymode	[0/1/2]		Display or set the encryption mode for SGMP messages. [0:NONE /1:DES/2:3DES] specifies the encryption mode to be set.
	keepalive			Display the time(second) to report agent keepalive 0: disable. Set the time(second) to report agent keepalive; the valid range : 10 ~ 2147483647
	version			Display the Vantage agent version.

Embedded RADIUS server (PEAP) Related Command

Command				Description
radServ	debug_level	radserv=[level]		Debug level of RADIUS module
		mschapv2=[level]		Debug level of MS-CHAPv2 module
	time_out	[time out value (ms)]		Time out value for one session (in millisecond)
	authenticator	Set	[entry_no] [active]	Activate/deactivate the authenticator of entry_no
			[entry_no] [active] [IP] [secret]	Set the information of the authenticator
		remove	[entry_no]	Remove authenticator of entry_no
		list		Show all the setting of authenticators

sys	logs	category	radius [0:none/1:log] [0:don't show debug type/1:show debug type]	Set centralized log for RADIUS enable/disable

Appendix 2: Embedded RADIUS server (PEAP)

1. Introduction

Security has always been one of the crucial issue of network connection. To assure information safety, the identities of the peers must be authenticated first. RADIUS stands for Remote Access Dial-In User Service, which has a database of all the peers and is responsible for authentication. The RADIUS server plays the role of the authentication server of an authentication protocol like IEEE 802.1X. Extensible Authentication Protocol (EAP) was first invented to deal with PPP link authentication. With its flexibility, EAP can carry almost every user authentication protocols, for example, PEAP (Protected EAP) and MD5-Challenge. Because of this advantage, IEEE 802.1X uses EAP on the link between supplicant and authenticator, and the RADIUS extension has set EAP as a standard attribute as well. To provide EAP with advanced security, engineers from Microsoft proposed PEAP that utilizes TLS (Transport Layer Security) to protect all the authenticating information. By embedding the RADIUS server in our APs (Access Points), customers can take advantage of better wireless security with lower cost than buying an extra standalone RADIUS server.

2. IEEE 802.1X

[IEEE Std 802.1X-2001] defines a mechanism for Port based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases where the authentication and authorization process fails.

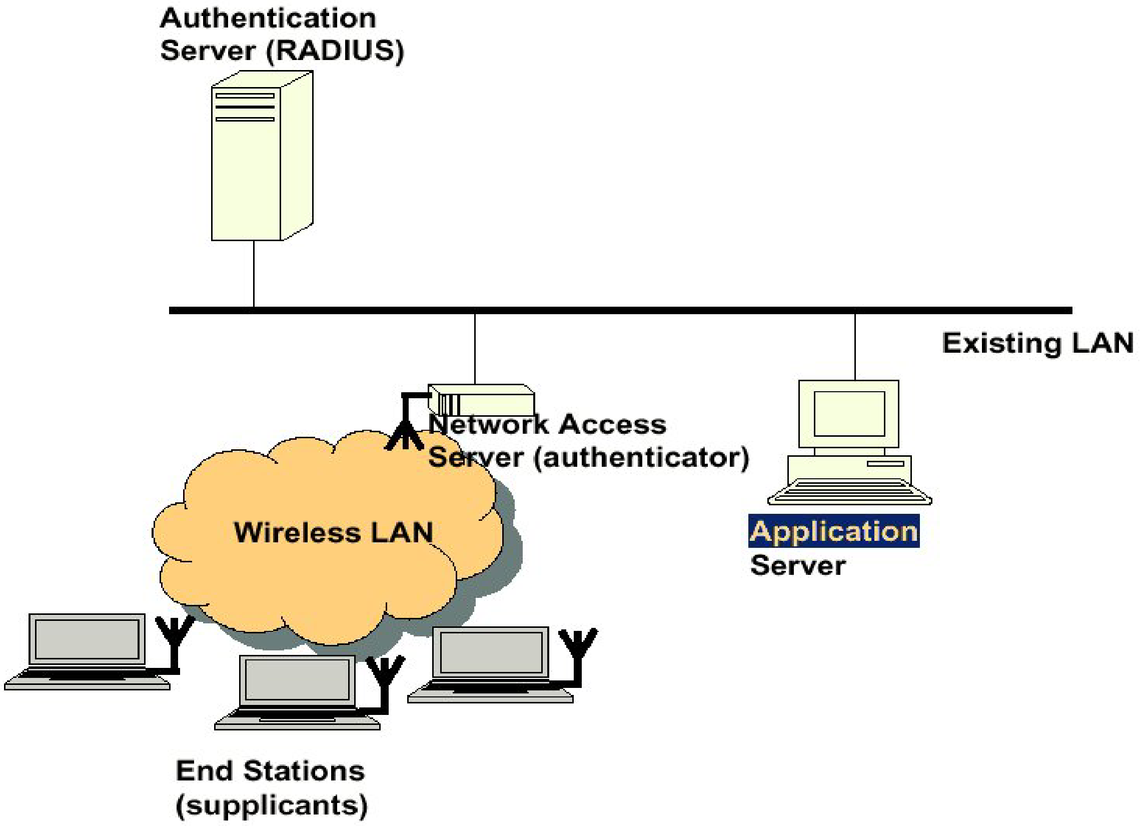
Authentication Server (RADIUS)
Existing LAN
Network Access Server (authenticator)
Wireless LAN
Application Server
End Stations (supplicants)

Figure 1. IEEE 802.1X

3. RADIUS

Remote Access Dial-In User Service or RADIUS is an access-control protocol that verifies and authenticates users based on the commonly used challenge/response method. While RADIUS has a prominent place among Internet service providers, it also belongs in any environment where central authentication, regulated authorization, and detailed user accounting is needed or desired.

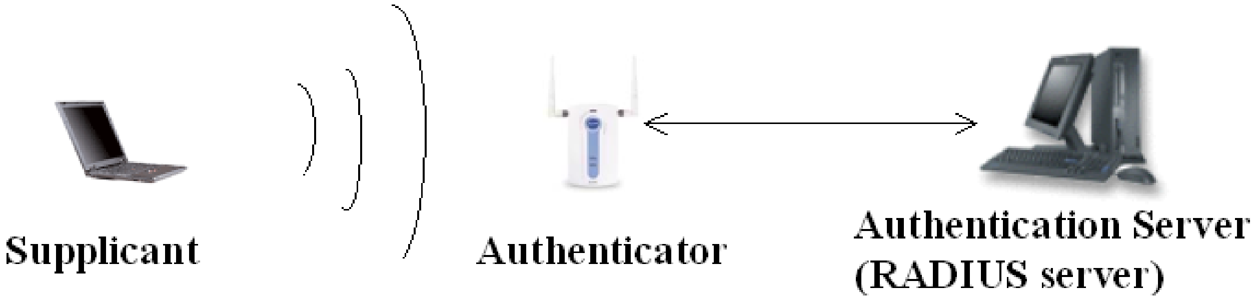

Figure 2. IEEE 802.1X w/ Standalone RADIUS server

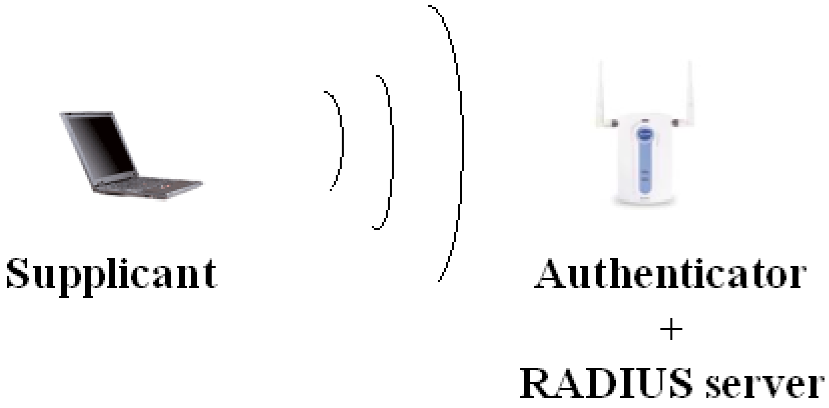

Figure 3. IEEE 802.1X w/ Embedded RADIUS server

4. EAP

Extensible Authentication Protocol (EAP) is a general protocol for authentication which supports multiple authentication mechanisms. EAP does not select any specific authentication mechanism at first. This allows the authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a “back-end” server which actually implements the various mechanisms while the authenticator merely passes through the authentication exchange.

5. PEAP

EAP was developed or used on wired networks, where physical security was presumed. Where an attacker can easily gain access to the medium (such as on a wireless network or where EAP is run over IP), the presumption of physical security is no longer valid. Since the EAP method negotiation is unprotected, an attacker can inject packets in order to cause the negotiation of a method with lesser security. Denial of service attacks are also possible. PEAP is an EAP type that addresses this security issue by first creating a secure channel that is both encrypted and integrity-protected with Transport Level Security (TLS). Then, a new EAP negotiation with another EAP type occurs, authenticating the network access attempt of the client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols that are normally susceptible to an offline dictionary attack can be used for authentication in wireless environments.

Appendix 3: Backup RADIUS server

ZyAIR devices support at most 5 backup radius servers and accounting servers setting. ZyAIR devices use the first radius server setting as the default configuration. Figure (1) shows the backup radius server concept. There are two radius servers can be reached by ZyAIR device. If supplicant issue an authentication request to ZyAIR device and trying to authenticate with radius server, ZyAIR device will keep trying forward this request to radius server 1. If ZyAIR device keep trying for 3 times and radius server still doesn't response the request then ZyAIR device will auto switch the authentication request packet to radius server 2. The trying time interval is depending on the supplicant re-try interval.

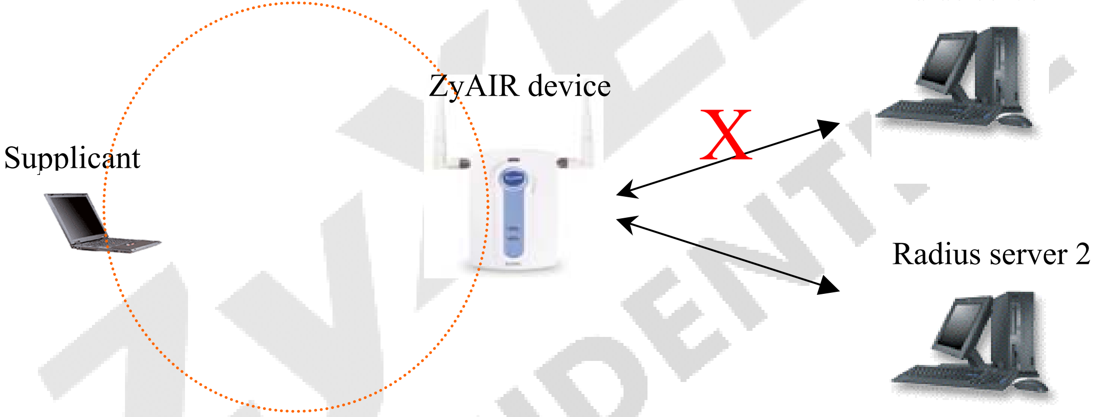

Figure (1)